**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF WEST VIRGINIA**
**AT CHARLESTON**

**UNITED STATES OF AMERICA**

**v.** **CRIMINAL ACTION NO. 2:14-00194**

**RONNIE EUGENE NAYLOR**

**MEMORANDUM OPINION AND ORDER**

Pending is defendant Ronnie Eugene Naylor's motion to suppress, filed January 6, 2015.

On January 20, 2015, the parties submitted a joint stipulation of fact. On January 21, 2015, the court held an evidentiary hearing attended by counsel for the parties and Mr. Naylor. The matter is now submitted for decision. The court summarizes the joint stipulation in subsection I.A below, supplemented by additional findings of fact and conclusions of law in subsection I.B.

I.

Sergeant David Eldridge is an investigator assigned to the West Virginia State Police Crimes Against Children Unit. He

uses a law enforcement software program known as the Child Protection System ("CPS"). The CPS software is designed to investigate the collection and distribution of child pornography by use of peer-to-peer software.[1] The CPS software was developed and managed by a private company called TLO, Inc. It is now managed by the Child Rescue Coalition. The CPS software allows law enforcement to search peer-to-peer networks for files containing terms associated with child pornography.

Image and video files containing depictions of child pornography can be identified by their hash value. A hash value is essentially a "digital fingerprint" unique to a particular file. The CPS software generates a network activity spreadsheet. The spreadsheet contains information on certain files purported to be available from peers, as well as the Internet Protocol address ("IP address") showing the location of the material.[2]

---

[1] The court notes that in such a system the referenced "peers" are understood to be computers linked over the Internet. The peers may then share files without need of a server. Each linked computer assumes the status of both a client and a server.

[2] An IP address is a numerical label assigned to a particular Internet connection used by one or more computers.

Sergeant Eldridge's investigation of this matter began on January 16, 2014. He reviewed a CPS spreadsheet for the IP address 184.14.34.185. The spreadsheet Sergeant Eldridge used contained, inter alia, the following types of information: (1) the IP address for the target computer, (2) a time stamp referring to the date and time a file was available on the target computer, (3) the file's hash value, (4) a Global Unique Identifier ("GUID") number[3], (5) the file name, (6) the file size, (7) the program being used for file sharing by the target, and (8) the file percentage available.

The spreadsheet showed a total of 29 digital media files putatively containing child pornography available for download from the suspect IP address on January 15 and 16, 2014. Sergeant Eldridge used the West Virginia State Police media library to compare the hash values of its holdings with the hash values for the 29 files. One file was entitled "Lolitas House 34 - Vika(13 Yo), Sasha (12Yo) & Luba (10Yo) - Lesbian -

[3] A GUID number is generated by the version of the peer-to-peer software program being used by a computer located at the suspect IP address. A GUID number is automatically created when a user installs or updates the software.

Sofabed.avi" ("Lolitas House"). The spreadsheet's SHA-1 hash[4] for this particular file was "B6UXAVNDAOFZY6XVMRCKCR4B2RSMM4JA".

The Lolitas House file was categorized as "child notable" on the CPS software spreadsheet reviewed by Sergeant Eldridge. The spreadsheet revealed that, on January 15, 2014, at 4:38 a.m. and 5:18 a.m., 25.52% of the Lolitas House file was available for distribution from the suspect IP address. The spreadsheet further showed that the entire Lolitas House file was available for distribution from the suspect IP address on January 16, 2014 at 4:18 a.m.

Sergeant Eldridge did not download any of the 29 files from the suspect IP address. He instead reviewed the copy of the Lolitas House file found in the media library. He learned that it was approximately 14 minutes and 48 seconds in length, with minors engaged in sexually explicit conduct. Specifically, he described it as a clip spanning 14 minutes and 48 seconds with three prepubescent females disrobing, displaying their genitalia, and engaging in various sexual activities including

[4] SHA-1 is a cryptographic hash function originating with the National Security Agency. Hash functions are, inter alia, used to ensure data integrity. SHA-1 is a Federal Information Processing Standard published by the United States National Institute of Standards and Technology.

lascivious exhibition of the genitals, masturbation and oral intercourse.

On April 10, 2014, Sergeant Talia Divita of the West Virginia State Police applied to a county magistrate judge for a search warrant. The targeted residence was in Elkview, West Virginia. The application alleged that persons at that address possessed material containing depictions of child pornography in violation of W.Va. Code, §61-8C-3. While not found in the joint stipulation, it appears undisputed that the material portions of the warrant application stated as follows:

> On [January 16, 2014], Sgt. D.C. Eldridge conducted a search of the Grid Cop database of . . . [IP] addresses that have been previously identified as being involved in the possession and trafficking of digital media files of child pornography.
>
> Sgt. D.C. Eldridge examined these records and located an . . . [IP] address associated with a computer believed to be in the vicinity of Walton, Roane County, West Virginia that had been previously identified through investigative processes as containing digital media files believed to be child pornography. This Internet Protocol address was identified as 184.14.34.185 and the GUID associated with the suspect computer was identified as CA4D2EE81BBA6E4481FE71FB7CEB68D5.
>
> The Grid Cop database further indicated that the user of . . . [IP] address 184.14.34.185 had been logged as being involved in the possession and distribution of 29 digital media files of child pornography.
>
> Sgt. D.C. Eldridge reviewed the hash values and file names associated with . . . [IP] address 184.14.34.185

**that were logged in the . . . [Internet Crimes Against Children ("ICAC")] database.**

**Of the media files logged from this IP address, Sgt. D.C. Eldridge examined exact copies of the following media file(s) and observed that these file(s) depicted minors engaged in sexually explicit conduct.**

**A digital video titled Lolitas House 34 - Vika (13Yo), Sasha (12Yo) & Luba (10Yo) -- Lesbian -- Sofabed.avi. This video is approximately 14 minutes and 48 seconds in duration. This video depicts three prepubescent females stripping their clothes off, displaying their genitalia and engaging in various sexual activities to include lascivious exhibition of the genitals, masturbation and oral intercourse.**

**Sgt. D.C. Eldridge reviewed the network activity associated with . . . [IP] address 184.14.34.185 and the above child pornography file and determined that this file had been offered [for] distribution by a computer using . . . [IP] address 184.14.34.185 on January 15, 2014 at 04:38:00 AM (GMT).**

**On this same date, Sgt. D.C. Eldridge determined that 184.14.34.185 was issued to Frontier Communications.**

**On this same date, Sgt. D.C. Eldridge obtained an Administrative Subpoena from Raleigh County, West Virginia Magistrate Steve Massey which directed . . . Frontier Communications to identify the subscriber information associated with the use of . . . [IP] address 184.14.34.185 on January 15, 2014 at 04:38:00 AM (GMT).**

**On this same date, Sgt. D.C. Eldridge served the above Administrative Subpoena to Frontier Communication via facsimile.**

**On January 17, 2014, Frontier Communications responded to this Administrative Subpoena and indicated that on January 15, 2014 at 04:38:00 AM (GMT), . . . [IP] address 184.14.34.185 was assigned to an internet service account issued to . . . [an individual at] 6182 Quick Road, Elkview, WV 25071.**

(Dckt. Ent. 23-2 at 17). The search warrant issued and, on April 10, 2014, Sergeant Divita executed it at the subject residence. Mr. Naylor was living at the residence at that time but was not present when the search occurred.

Two computers were seized. A Seagate 500 GB hard drive taken from a computer attributed to Mr. Naylor was subsequently examined forensically by Corporal Robert Boggs, who oversees the West Virginia State Police Digital Forensics Unit. The hard drive contained two images and 132 video files constituting suspected depictions of child pornography. Corporal Boggs was unable, however, to show that the Lolitas House file was present. In sum, there is no trace of the Lolitas House file on Mr. Naylor's hard drive.

On April 15, 2014, Mr. Naylor submitted to a non-custodial interview with Sergeant Divita at the West Virginia State Police Detachment in South Charleston, West Virginia. The statement was digitally recorded.

On September 10, 2014, the United States filed a single-count indictment alleging that Mr. Naylor, on or about April 10, 2014, possessed child pornography in violation of 18 U.S.C. § 2252(a)(5)(B) and 2252A(b)(2). On January 27, 2015,

the United States filed a superseding indictment alleging, in addition to the original charge (now Count Three), that Mr. Naylor, on or about March 15 and 29, 2014, respectively, knowingly received child pornography (Counts One and Two), in violation of 18 U.S.C. § 2252(a)(5)(B) and 2252A(b)(1).

In the instant motion to suppress, Mr. Naylor seeks exclusion of both the evidence seized and any tainted incriminating statements volunteered by Mr. Naylor. He asserts suppression is warranted based upon a number of considerations: (1) Sergeant Eldridge failed to download the Lolitas House video which would have confirmed its content and availability for download, (2) the CPS program has not been shown to warrant the reliance placed upon it by law enforcement in establishing probable cause, (3) the Lolitas House video was not found during a forensic examination of Mr. Naylor's hard drive, (4) only 25.52% of the Lolitas House video was shown on the spreadsheet, indicating a false statement is found in the warrant application, (5) there was no way for Sergeant Eldridge to ascertain if the 25.52% included child pornography, and (6) there was no independent judicial assessment made to determine probable cause inasmuch as there were no photocopies or screen captures of any suspect video files.

**B. Additional Findings of Fact**

**Sergeant Eldridge has used the CPS software since 2009. Fifty of the child pornography cases to which he has been assigned have involved use of the CPS software. He has found it to be 100% reliable. In summary, the CPS program works by listening over, and performing searches on, Internet networks. In doing so, it attempts to find those users offering, or desiring, results associated with child exploitation. As responses are received by the CPS software, they are logged. It is the fruits of these logging efforts that results in the type of spreadsheet reviewed by Sergeant Eldridge in this action.**

**The media library maintained by the West Virginia State Police consists of 70,000 child pornography files collected over the years. In addition to finding a hash-value match for the Lolitas House video in the media library, Sergeant Eldridge also found another file on the spreadsheet related to the suspect IP address that matched an additional archived file in the repository. Respecting hash values, a file hash is able to identify a particular file with accuracy on the order of DNA typing or fingerprinting.**

The Lolitas House file contained only one minute and 32 seconds of material that did not constitute child pornography. The 25.52% available for distribution on January 15, 2014, constitutes in excess of three minutes of its running time.

## II.

### A. Governing Standards

The Fourth Amendment provides that "[t]he right of the people to be secure in their . . . houses . . . against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . . " U.S. Const. amend. IV; see United States v. Rumley, 588 F.3d 202, 205 (4th Cir. 2009).

Longstanding Supreme Court precedent teaches that "probable cause is a fluid concept -- turning on the assessment of probabilities in particular factual contexts." Illinois v. Gates, 462 U.S. 213, 232 (1983). The standard requires "only the probability, and not a prima facie showing, of criminal activity" under the totality of the circumstances. Id. at 235;

see id. at 238 ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.") (internal quotations omitted).

A reviewing court must bear in mind that "affidavits are normally drafted by nonlawyers in the midst and haste of a criminal investigation." Gates, 462 U.S. at 235. It is for this reason that "[t]echnical requirements of elaborate specificity once exacted under common law pleading have no proper place in this area." Id. (internal quotations omitted). It is not the function of an issuing judicial officer "to require that the affiant amass every piece of conceivable evidence before seeking a warrant . . . ." See United States v. Montieth, 662 F.3d 660, 665 (4th Cir. 2011) (citations omitted).

B. Analysis

As noted, the warrant application included Sergeant Divita's sworn statement that her colleague, Sergeant Eldridge,

had examined an exact copy of the Lolita's House file in the media library and found it to contain minors engaged in sexually explicit conduct. The file content is described with particularity. Respecting the availability of the file for download by other peers, Sergeant Eldridge noted it had been offered for distribution by the target computer on January 15, 2014. These allegations produced a fair probability that contraband or evidence of a crime would be found on the target computer.

None of Mr. Naylor's challenges cast any doubt on this conclusion. First, the fact that Sergeant Eldridge failed to download the Lolitas House video is of no moment. Based upon a garden-variety knowledge of hash value characteristics, he was warranted in concluding that the Lolitas House video was an exact match for the same file archived in the media library, a file that contained a profound amount of child pornography.

Second, a sufficient showing has been made to warrant Fourth Amendment confidence in the CPS software. Sergeant Eldridge has used the CPS software for six years. Fifty of the hundreds of child pornography cases to which he has been assigned have involved use of the CPS software. On those occasions, the CPS software has proven to be 100% reliable.

**There is simply no basis to challenge the integrity of the software in light of this track record. The CPS software appears to be a reliable investigative tool for law enforcement in these types of cases.**

**Third, it is of no consequence that the Lolitas House video was not found during a forensic examination of Mr. Naylor's hard drive. There are multiple reasons that the file may have disappeared. It could have been deleted and then overwritten or moved, directly or following download, to an external storage device. The absence of the file does not diminish the showing of probable cause.**

**Fourth, the fact that only 25.52% of the Lolitas House video was shown on the spreadsheet on January 15, 2014, does not indicate Sergeant Eldridge or Sergeant Divita made a recklessly false statement within the warrant application. Inasmuch as another user may begin downloading a fellow user's partially downloaded file, there is no basis for concluding any statement in the warrant application misstated or stretched the truth. In a related vein, Sergeant Eldridge could confidently conclude that 25.52% of the file included child pornography inasmuch as that portion of the file would have captured at least some measure of child pornography based upon his percentage**

allocation after viewing the exact duplicate of the file in the media library.[5]

Accordingly, it is ORDERED that Mr. Naylor's motion to suppress be, and hereby is, denied.[6]

The Clerk is directed to transmit a copy of this written opinion and order to the defendant and counsel of record.

ENTER: February 19, 2015

John T. Copenhaver, Jr.
United States District Judge

[5] Mr. Naylor additionally asserts as follows: "Where this defendant has no legal grounds within this Circuit to submit a staleness challenge to Sgt. Divita's application, the Government should bear the burden of producing sufficient forensic evidence which demonstrates the current or former presence of the identified contraband file being located on a subsequently seized computer." (Def.'s Reply at 4). The court need not reach the suitability of the broad rule advanced by Mr. Naylor in light of the foregoing analysis.

[6] Mr. Naylor additionally relies upon the court of appeals' decision in United States v. Doyle, 650 F.3d 460 (4th Cir. 2011). The circumstances in Doyle were much different than this case for a number of reasons. For example, it was revealed during a suppression hearing that the officer who signed the warrant application and the supporting affidavit was uninvolved in the investigation. Also lacking was a description of the nexus between the place to be searched and the items to be seized, the date(s) that the alleged child pornography was possessed, or a description of the alleged illegal child pornography beyond the notation that defendant possessed pictures of nude children. The decision in Doyle is inapposite.